National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

FIPS 140-3

Section 5 – Physical Security

Randall J. Easter

Director, NIST CMVP

Ken Lu

CSE CMVP

September 28, 2005

Agenda

- Overview
- New Embodiments
- New Levels
- New requirements

FIPS 140-3: Security Areas

1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Authentication, and Services
4. Software Security
5. **Physical Security**
6. Operational Environment
7. Sensitive Security Parameter (SSP) Management
8.
9. Self Tests
10. Implementation Assurance
11. Mitigation of Other Attacks

Section 5 – Physical Security

- A cryptographic module **shall** employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module (including substitution of the entire module) when installed. All hardware, software, and data components within the cryptographic boundary **shall** be protected.
- Depending on the physical security mechanisms of a cryptographic module, unauthorized attempts at physical access, use, or modification will have a high probability of being detected
  - subsequent to an attempt by leaving visible signs (i.e., tamper evidence)

    and/or

  - during an access attempt so that appropriate immediate actions can be taken by the cryptographic module to protect CSPs and PSPs (i.e., tamper response). Immediate actions **shall** be taken to mean that retrieval of CSPs and PSPs are not possible.

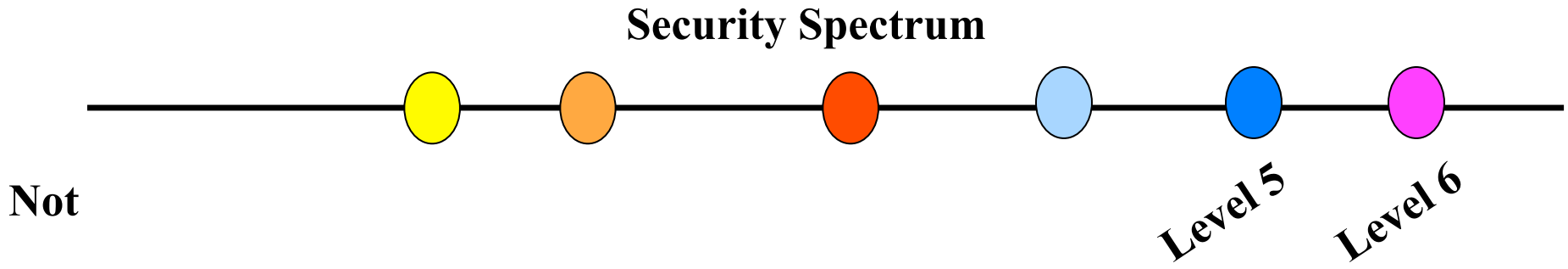
Embodiments

- ***Sub-Chip cryptographic modules*** are physical embodiments in which a region or part of a single integrated circuit (IC) chip constitutes the cryptographic module. An example of a sub-chip cryptographic module would be a complex single IC chip containing a distinct separate microprocessor, memory devices (e.g. RAM, EEPROM, FLASH) that may also includes a separate distinct cryptographic module.
- ***Single-chip cryptographic modules*** are physical embodiments in which a single integrated circuit (IC) chip may be used as a standalone device or may be embedded within an enclosure or a product that may not be physically protected. Examples of single-chip cryptographic modules include single IC chips or smart cards with a single IC chip.
- ***Multiple-chip embedded cryptographic modules*** are physical embodiments in which two or more IC chips are interconnected and are embedded within an enclosure or a product that may not be physically protected. Examples of multiple-chip embedded cryptographic modules include adapters and expansion boards.
- ***Multiple-chip standalone cryptographic modules*** are physical embodiments in which two or more IC chips are interconnected and the entire enclosure is physically protected. Examples of multiple-chip, standalone cryptographic modules include encrypting routers or secure radios.

Table 2: Summary of physical security requirements

	General Requirements for all Embodiments	Sub-Chip Cryptographic Module	Single-Chip Cryptographic Modules	Multiple-Chip Embedded Cryptographic Modules	Multiple-Chip Standalone Cryptographic Modules
Security Level 1	Production-grade components	No additional requirements.	No additional requirements.	If applicable, production-grade enclosure or removable cover.	Production-grade enclosure.
Security Level 2	Evidence of tampering Opaque covering	Opaque tamper-evident coating on chip or enclosure.	Opaque tamper-evident coating on chip or enclosure.	Opaque tamper-evident encapsulating material or opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.
Security Level 3	Tamper response and zeroization circuitry Vents protected from probing Simple Power Analysis Protection	Hard opaque tamper-evident coating on chip or strong opaque removal-resistant and penetration resistant enclosure.	Hard opaque tamper-evident coating on chip or strong opaque removal-resistant and penetration resistant enclosure.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multiple-Chip Standalone Security Level 3 requirements.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong opaque enclosure with removal/penetration attempts causing serious damage.
Security Level 4	No additional requirements	Hard opaque removal-resistant coating on chip.	Hard opaque removal-resistant coating on chip.	Tamper detection envelope with tamper response and zeroization capability.	Tamper detection envelope with tamper response and zeroization capability.
Security Level 5	EFP or EFT for temperature and voltage EMI Protection	No additional requirements.	No additional requirements.	No additional requirements.	No additional requirements.
Security Level 6	Differential Power Analysis Protection	No additional requirements.	No additional requirements.	No additional requirements.	No additional requirements.

FIPS 140-2: Security Levels



- Level 1 is the lowest, Level 6 most stringent
- Requirements are primarily cumulative by level
- Overall rating is lowest rating in all sections
- Validation is applicable when a module is configured and operated in accordance with the level to which it was tested and validated

General Physical Security Requirements

- The following requirements **shall** apply to all physical embodiments and levels.
  - Documentation **shall** specify the physical embodiment and the security level for which the physical security mechanisms of a cryptographic module are implemented.
  - Documentation **shall** specify the physical security mechanisms of a cryptographic module.

General Physical Security Requirements
Level 1

- The cryptographic module **shall** consist of production-grade components that **shall** include standard passivation techniques (e.g., a conformal coating or a sealing coat applied over the module's circuitry to protect against environmental or other physical damage).

General Physical Security Requirements
Level 2

- The cryptographic module **shall** provide evidence of tampering (e.g., on the cover, enclosure, and seal) when physical access to the module is attempted.
- The cryptographic modules components **shall** be opaque.
  - If the cryptographic module contains ventilation holes or slits, internal components **shall** be protected from observation.

General Physical Security Requirements
Level 3

- If the cryptographic module contains any doors or removable covers or if a maintenance access interface is defined, then the module **shall** contain tamper response and zeroization circuitry. The tamper response and zeroization circuitry **shall** immediately zeroize all plaintext secret and private keys and CSPs when a door is opened, a cover is removed, or when the maintenance access interface is accessed. The tamper response and zeroization circuitry **shall** remain operational when plaintext secret and private cryptographic keys or CSPs are contained within the cryptographic module.

- If the cryptographic module contains ventilation holes or slits, then the holes or slits **shall** be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g., require at least one 90 degree bend or obstruction with a substantial blocking material).

- The cryptographic module **shall** be designed to protect against simple power analysis attacks.

General Physical Security Requirements
Level 4

- The cryptographic module **shall** be protected by a hard opaque removal-resistant coating, or

- The cryptographic module **shall** be protected by a tamper detection envelope with tamper response and zeroization capability.

General Physical Security Requirements **Level 5**

- The cryptographic module **shall** either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT) as specified in Section 4.5.5, and

- The cryptographic module **shall** include protection against Electromagnetic attacks (EMA).

General Physical Security Requirements
Level 6

- The cryptographic module **shall** be designed to protect against differential power analysis and differential electromagnetic analysis attacks.

Areas of Discussion

- Physical security section split into two types of attacks
  - Invasive
    - Defeating physical protection mechanisms
  - Non-invasive
    - Acquiring CSPs via external mechanisms

Areas of Discussion

- Invasive
  - Level 1
    - No protection
  - Level 2
    - Tamper evidence, opaqueness
  - Level 3
    - Active zeroization for removable covers and doors
    - Ventilation holes/slits allowed but inhibited via 90 degree baffles
    - Strong enclosures, hard opaque epoxy
    - EFT: +/- 20% of operating envelope
    - Protection from fault induction
    - Ionizing Radiation
  - Level 4
    - Encapsulated in tamper responding cocoon with a degree of difficulty of penetration
    - Ventilation holes/slits allowed but inhibited via 180 degree baffles
    - EFP/EFT: -100C to +200C
  - Level 5
    - Encapsulated in tamper responding cocoon with a high degree of difficulty of penetration
    - Probing prevented
  - Level 6
    - ??

Areas of Discussion

- Non-Invasive (Side-Channel) *Optional – Required Level 4*
  - ❑SPA 1 2 3 4 5
  - ❑EMA 1 2 3 4 5
  - ❑DPA 1 2 3 4 5
  - ❑DEMA 1 2 3 4 5
  - ❑Timing 1 2 3 4 5
  - ❑Annex X 1 2 3 4 5

Areas of Discussion

- CMT Laboratory Testing Methods
  - SPA, DPA, DEMA
  - Fault Induction
- Ionizing radiation attack protection?
- Other physical protection mechanisms
- Technology dependencies
  - Single Chip …. Sub-chip …. SmartCard

Areas of Discussion

- New informative Annex
  - Provide user community with attack protection rationale
- Provide lifecycle security requirements or guidance from manufacturing to scrap
- Require external security controls to be included in Security Policy
- Standardized chemical testing suites
- Replacement of tamper evident labels
- Security Policy requirements for post error/tamper recovery
- Penetration Testing/Vulnerability Analysis at Level 7

Additions to Standard

things to consider

- Must provide method for conformance testing
  - CMVP is not a evaluation process
- Should not be device type specific
- Should not involve long, difficult and costly testing
  - Shall be timely and cost effective
  - Exception may be at higher levels

NIST

- **Randall J. Easter** – Director, CMVP, NIST
  reaster@nist.gov

CSE

- **Ken Lu** – Technical Authority, CMVP, CSE
  ken.lu@CSE-CST.GC.CA